

ABSTRACT

A network interface system is presented for interfacing a host system with a network, including a bus interface system, a media access control system, a memory system, a security system, and a descriptor management system, wherein the descriptor management system obtains initialization vector information from the host system and provides the initialization vector information to the security system. A method of encrypting outgoing data in a network interface system is provided, comprising providing initialization vector information from a descriptor to a security system in a network interface system, selectively encrypting or authenticating outgoing data using the security system, and selectively employing an initialization vector from the outgoing data to perform CBC encryption of the outgoing data according to the initialization vector information.